Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. – 4. (canceled)

5. (currently amended) A tamper-resistant processing method comprising the steps of:

(a) deciding whether to first transfer one operation unit in the bit pattern of data A in a memory to a first register R1 and then to transfer one operation unit in the bit pattern of data B in the memory to a second register R2, or to first transfer one operation unit in the bit pattern of said data B to said second register R2 and then to transfer one operation unit in the bit pattern in said data A to said first register R1;

(b) transferring each operation unit to said registers R1 and R2, respectively, in accordance with the order of transfer decided in step (a);

~~(b)~~ (c) executing a predetermined arithmetic operation on the contents of said first register R1 and the contents of said second register R2;

~~(c)~~ (d) storing the result of said arithmetic operation in the memory,

~~(d)~~ (e) repeating the steps from (a) through ~~(c)~~ (d) until said arithmetic operation for said data A and said data B is finished.

6. (currently amended) A tamper-resistant processing method comprising the steps of:

(a) deciding whether to first transfer one operation unit of data A in a memory to a first register R1 and then to transfer one operation unit of data B in the memory to a second register R2, or to first transfer said one operation unit of the data A to said second register R2 and then to transfer said one operation unit of the data B to said first register R1;

(b) transferring each operation unit to said registers R1 and R2, respectively, in accordance with the order of transfer decided in step (a);

~~(b)~~ (c) executing a predetermined arithmetic operation on the contents of said first register R1 and on the contents of said second register R2;

~~(c)~~ (d) storing the result of said arithmetic operation in the memory;

~~(d)~~ (e) repeating the steps from (a) through ~~(c)~~ (d) until said arithmetic operation on said data A and said data B is finished.

7. (previously presented) A tamper-resistant processing method of claim 6 wherein whether to first transfer one operation unit of the data A to said first register R1 or to said second register R2 is determined with the use of a generated random number.

8. (original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is the operation for an arithmetic sum.

9. (original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is the operation for an arithmetic product.

10. (original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is any one of the logical sum OR, logical product AND, and exclusive logical sum EXOR.

11. – 13. (canceled)